

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-112796

(43) Date of publication of application : 21.04.2000

G06F 17/30

(72)inventor : O FLAHERTY KENNETH W
STELLWAGEN RICHARD G JR
WALTER TODD A
WATTS REID M
RAMSAY DAVID A
ADRIAN W BELDHUISEN
RENDA K OZDEN
PATLARICK B DEMPSTER

Priority number : 98 165777 ???? Priority date : 02.10.1998 ???? Priority country : US

(54) METHOD AND SYSTEM FOR MANAGING DATA PRIVACY IN DATABASE MANAGEMENT SYSTEM

PROBLEM TO BE SOLVED: To give the whole advantages given by the system while paying attention to privacy by controlling access to data according to a privacy parameter.

[illegible]

LEGAL STATUS

28.09.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-112796
(P2000-112796A)

(43) 公開日 平成12年4月21日 (2000.4.21)

(5) IntCl ⁷	識別番号	F I	データコード (参考)
G 0 6 F 12/00	5 1 2	G 0 6 F 12/00	5 1 2
	5 3 7		5 3 7 A
12/14	3 1 0	12/14	3 1 0 K
17/30		15/40	3 2 0 B

審査請求 未請求 請求項の数27 O L (全 20 頁)

(21) 出願番号 特願平11-281593

(22) 出願日 平成11年10月1日 (1999.10.1)

(31) 優先権主張番号 09/165777

(32) 優先日 平成10年10月2日 (1998.10.2)

(33) 優先権主張国 米国 (US)

(71) 出願人 592089054

エヌシーアール インターナショナル インコーポレイテッド
NCR International, Inc.
アメリカ合衆国 45479 オハイオ、デイトン サウス バタソン プールバード 1700

(74) 代理人 100098589

弁理士 西山 善章

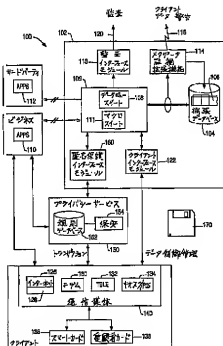
最終頁に続く

(54) 【発明の名称】 データベース管理システムにおけるデータプライバシー管理の方法およびシステム

(57) 【要約】

【目的】 データベース管理システムにおけるデータプライバシーを管理する方法、装置および製造方法を提供する。

【構成】 本装置は、複数のデータベース表にデータを格納すると共にその表からデータを取り出すためのデータベース管理システムを含む。このデータベース表内のデータは、データベース表に格納されているプライバシーパラメータにしたがって制御可能にアクセスすることができる。本装置はまたデータベース管理システムインターフェースを含み、このインターフェースはデータベース管理システムに作動上結合されており、プライバシーパラメータにしたがってデータベース表内のデータのアクセスを制御する。本装置はさらに監査モジュールを含む。このモジュールはデータベース管理システムインターフェースと通信できるように結合されており、データベース管理システム内のデータプライバシーパラメータが有効に適用できるようにする。



【特許請求の範囲】

【請求項1】 複数の行および列にデータを格納する複数のデータベース表にデータを格納し、その表からデータを取り出すデータベース管理システムにして、該データベース表に格納されているブライバシーパラメータにしたがって該データベース表のデータが制御可能にアクセスできる、データベース管理システムと、

該データベース管理システムに動作上結合されており、該ブライバシーパラメータにしたがって該データベース表内のデータへのアクセスを制御する、データベース管理システムインターフェースと、

を含むことを特徴とする、データウェアハウス化兼管理策ブライバシー制御システム。

【請求項2】 該データベース管理システム内の該データブライバシーパラメータの適用を有効にするため、該データベース管理システムインターフェースと通信すべく結合された監査モジュールに含むことを特徴とする、請求項1に記載のシステム。

【請求項3】 データソースと該データベース表へアクセスする主体との間の通信を匿名化するため、データソースにより選択的に呼び出すことが可能な信託プロキシサービスをさらに含むことを特徴とする、請求項2に記載のシステム。

【請求項4】 該データベース管理システムインターフェースに動作上結合されており、データソースからデータブライバシープレファレンスデータを受信すると共に該データブライバシープレファレンスデータを該データベース管理システムインターフェースに与える手段を含む、データソースインターフェースモジュールをさらに含むことを特徴とする、請求項2に記載のシステム。

【請求項5】 該データソースインターフェースモジュールがさらに、該データベース管理システムからブライバシーパラメータを取得すると共に該ブライバシーパラメータを該データソースに与える手段を含むことを特徴とする、請求項4に記載のシステム。

【請求項6】 データソースの固有の固定データおよび通信保安情報格納しているブライバシーデバイスを受信するためのデータソースサービスマジュールをさらに含むことを特徴とする、請求項2に記載のシステム。

【請求項7】 ブライバシーデバイスを受信する該手段がさらにブライバシーデータベースを発行する手段を含むことを特徴とする、請求項6に記載のシステム。

【請求項8】 当該データに対するブライバシーパラメータを集合的に記述するブライバシーデータを格納するブライバシー制御列が該データベース表に増加されることを特徴とする、請求項2に記載のシステム。

【請求項9】 フィールドを含むブライバシー制御列であってそのフィールドがそのフィールドに関連するデータに適用されるブライバシーパラメータを格納するようにされたブライバシー制御列が該データベース表に増

加されることを特徴とする、請求項8に記載のシステム。

【請求項10】 該データベース管理システムが、該データベース管理システムから送られるすべてのデータが通過する複数の強制データビューを有するデータビューシートを含むことを特徴とする、請求項2に記載のシステム。

【請求項11】 該データベース管理システムが、データリクエストをデータベース照会に翻訳するマクロシートを含むことを特徴とする、請求項2に記載のシステム。

【請求項12】 該監査モジュールが、該データベース管理システムインターフェースの現在時点における一貫性を監査することを特徴とする、請求項2に記載のシステム。

【請求項13】 データベース表内に格納されているデータに対するブライバシーパラメータの格納と取り出しを行うため該データベース表を拡張するステップにして、該データに関連する複数のデータベース表の列内に集合的に該ブライバシーパラメータが格納されるステップと、

該データソースからブライバシーパラメータを受信するステップと、

該データに関連する列に該ブライバシーパラメータを格納するステップと、

個人ブライバシーパラメータにしたがってデータベース管理システムインターフェースを介してのみ、該データベース表内のデータへのアクセスをリクエスト主体に与えるステップと、

該データベース表へのアクセスをアクセスログ (access log) 内に記録するステップと、

を含むことを特徴とする、データウェアハウス化兼ブライバシー制御システム内のデータソースから得られるデータを管理する方法。

【請求項14】 該アクセスログが、該データへのアクセスを来すSQLステートメントを含むアクセスデータを含むことを特徴とする、請求項13に記載の方法。

【請求項15】 該データベース表内のデータへのアクセスを与える該ステップが、リクエスト主体からデータリクエストを受信するステップと、

該リクエスト主体の身元に基づいて選択されるデータビューを与えるステップにして、該データビューが匿名化データビューおよび直用除外選択データビューを含むデータビュー群から選択されるようにされたステップと、を含むことを特徴とする請求項13に記載の方法。

【請求項16】 該データベース表内のデータへのアクセスを与える該ステップが、リクエスト主体からデータリクエストを受信するステップと、

該リクエスト主体の身元に基づいて選択されるマクロを与えるステップと、を含むことを特徴とする請求項13に記載の方法。

【請求項17】 該個人的プライバシーパラメーターが適用除外選択デフォルト値を含むことを特徴とする、請求項13に記載の方法。

【請求項18】 信託プロキシサービス内のデータソースから、トランザクション主体の身元データを含むプロキシサービスリクエストを受信するステップと、該データソースと該トランザクション主体との間の通信を匿名化するステップと、をさらに含むことを特徴とする請求項13に記載の方法。

【請求項19】 該データソースからアクセスリクエストメッセージを受信するステップと、該データソースの個人プライバシーパラメーターへのアクセスを与えと共に該データソースの個人プライバシーパラメーターへの変更を許す特権データビューを該データソースに与えるステップと、をさらに含むことを特徴とする請求項13に記載の方法。

【請求項20】 コンピューターによる読み取りが可能であり、該コンピューターにより実行可能な一つ以上の命令を実行してデータウェアハウス化兼プライバシー制御システム内のデータを管理する方法ステップを行うためのプログラム格納デバイスであって、該方法ステップが、

データベース表内に格納されているデータに対するプライバシーパラメーターの格納と取り出しを行うため該データベース表を拡張するステップにして、該データに関連する複数のデータベース表の列内に集合的に該プライバシーパラメーターが格納されるステップと、

該データソースからプライバシーパラメーターを受信するステップと、

該データベース表の列に該個人プライバシーパラメーターを格納するステップと、

個人プライバシーパラメーターにしたがってデータベース管理システムインターフェースを介してのみ、該データベース表内のデータへのアクセスをリクエスト主体に与えるステップと、

該データベース表へのアクセスをアクセスログ(access log)内に記録するステップと、を含む方法であることを特徴とする、プログラム格納装置。

【請求項21】 前記プログラム格納デバイスにおいて、該アクセスログが該データへのアクセスを来すSQLステートメントを含むことを特徴とする、請求項20に記載のプログラム格納装置。

【請求項22】 該データベース内のデータへのアクセスを与える該方法ステップが、

リクエスト主体からデータリクエストを受信するステップと、

該リクエスト主体の身元に基づいて選択されるデータビ

ューを与えるステップにして、該データビューが匿名化データビューおよび適用除外選択データビューを含むデータビュー群から選択されるようにされたステップと、を含む方法であることを特徴とする、請求項20に記載のプログラム格納装置。

【請求項23】 該データベース内のデータへのアクセスを与える該方法ステップが、

リクエスト主体からデータリクエストを受信するステップと、

該リクエスト主体の身元に基づいて選択されるマクロを与えるステップと、を含む方法であることを特徴とする、請求項20に記載のプログラム格納装置。

【請求項24】 該個人的プライバシーパラメーターが適用除外選択デフォルト値を含むことを特徴とする、請求項20に記載のプログラム格納装置。

【請求項25】 該方法ステップが、

信託プロキシサービス内のデータソースから、トランザクション主体の身元データを含むプロキシサービスリクエストを受信するステップと、

該データソースと該トランザクション主体との間の通信を匿名化するステップと、を含む方法であることを特徴とする、請求項20に記載のプログラム格納装置。

【請求項26】 該方法ステップが、

該データソースからアクセスリクエストメッセージを受信するステップと、

該データソースの個人プライバシーパラメーターへのアクセスを与えと共に該データソースの個人プライバシーパラメーターへの変更を許す特権データビューを該データソースに与えるステップと、を含む方法であることを特徴とする、請求項20に記載のプログラム格納装置。

【請求項27】 複数の行および列にデータを格納する複数のデータベース表にデータを格納しその表からデータを取り出すためのデータベース管理システムにして、該データベースに格納されているプライバシーパラメーターにしたがって該データベース表内のデータが制御可能にアクセスできる、データベース管理システムと、プライバシーデータを登録すると共にデータ、ユーザーおよびデータの使用するすべてを統括し、かつ該プライバシーパラメーターにしたがって該データベース表内のデータへのアクセスを制御する、プライバシーメタデータシステムと、を含むことを特徴とする、データウェアハウス化兼管理兼プライバシー制御システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はデータのウェアハウス(倉庫)化および解析の方法およびシステムに関し、特にデータベース管理システムにプライバシー制限を課する方法およびシステムに関する。

【0002】

【従来の技術】データベース管理システムはデータを収集、配布、および解析するのに使われる。このような大規模統合データベース管理システムは大量のデータを格納し、取出し、解析するための、効率的で一貫したかつ安全にデータのウェアハウス化を行う能力を提供する。大量の情報を収集、解析および管理を行うこの能力は、今日のビジネス界においてほぼ必須のものとなっている。

【0003】これらのデータウェアハウスに格納される情報は種々のソースから到来しうる。一つの重要なデータウェアハウス化アプリケーションはビジネス機関と消費者との間の商取引の過程で収集される情報の収集および解析を行う。例えば、ある個人が小売店である物品を購入するためにクレジットカードを使用すると、顧客の購入、購入物品、購入額その他の関連情報が収集される。従来、このような情報は当該取引を完了すべきか否かを決定するため、および製品在庫を制御するために小売業者が使用している。そのようなデータはまた、現在の購入傾向および地域的購入傾向を決定するのに使用することができる。

【0004】他の産業界でも個人データの使用が同様に行われている。例えば、銀行業務においては顧客の購買パターンはそのクレジットカード取引プロファイルまたは当座/預金口座の活動を解析することにより予測することができ、またある種のプロファイルをもつ顧客達は抵当か個人的退職者口座のような新規サービスを求める潜在的顧客として同定することができる。さらに、通信産業界では、通話記録から消費者通話パターンを解析することができ、ある種のプロファイルをもつ個人を2本目の電話線あるいはコールウェイテリングのような更新サービスの販売の対象として特定することができる。

【0005】さらに、データウェアハウス保有者は、普通、取引データを豊かにするためのデータをサードパーティー（第三者）から購入する。この豊富化のプロセスは家族構成、収入、雇用主、その他の個人データなどの人口統計データを豊かにする。

【0006】そのような取引期間中に収集されたデータは他の用途にも有用である。例えばある特定の取引に関する情報は当該消費者についての個人情報（年齢、職業、居住地、収入等）に相関づけて統計的情報を発生させることができる。ある場合にはこの個人情報は大まかに、当該消費者の身元（identification）を表す情報とそうでない情報との二つのグループに分類することができる。消費者の身元を表さない情報は有用である。なぜならばそれが類似の個人的特徴をもつ消費者達の購入傾向に関する情報を得るのに使用することができるからである。消費者の身元を表す個人情報により絞り込んだ個人的市場戦略に使用することができる。その場合、各個人消費者の購入習慣が解析されて別の市場の候補者あるいはある好みに合わせて半直した市場の候補者が同定

される。

【0007】個人データの収集が増大している別の例は、最近の「会員制」カードあるいは「愛顧者」カードの繁栄に現れている。これらのカードはある種の製品について顧客に割引価格を提供する。しかし顧客がそのカードを購入に使用する度に、顧客の購入習慣に関する情報が収集される。オンライン環境あるいはスマートカード、電話カードおよび借入カードすなわちクレジットカードでも同じ情報が得られる。

【0008】そのようなデータの収集および解析が大きな大衆的利益になりうるものの、それは残念ながらかなり悪用される対象ともなりうる。愛顧者プログラムの場合、かかる悪用の可能性が、本来は協力的な多数の消費者が会員費やその他のプログラムを得るのに参加することを阻害しかねない。またかかる悪用はキャッシュカードのような将来的技術を使用することを拒ませ、現金および小切手のようなより保守的な支払方法を継続することを助長する。実際、プライバシーに関する公衆の心配が、ウェブ商業が爆発的成長するとの期待を遅らせている要因であると信ぜられる。

【0009】これらすべての理由から、通常の制約と同様、個人情報データウェアハウスに格納されるとき、データを制御する者達はそのような悪用からデータを保護することを要求される。このコンピュータ時代において、データが益々収集されるにつれて個人に関するデータの使用上、個々人の権利が益々重要になっている。

【0010】

【発明が解決しようとする課題】本発明の課題は、消費者のプライバシーに対する関心に注意を払いつつ、完備したデータウェアハウスシステムを与えうるすべての利点を与えるシステムおよび方法を提供することである。

【0011】

【課題を解決するための手段】本発明はその第一の局面から見ると、データウェアハウス化兼管理兼プライバシー制御を行うシステム（data warehousing, management, and privacy control system）であって、複数の行および列にデータを格納する複数のデータベース表にデータを格納し、またその表からデータを取り出すデータベース管理システムにして、該データベース表に格納されているプライバシーパラメータにしたがって該データベース表のデータが制御可能にアクセスできる、データベース管理システム（database management system）と、該データベース管理システムに動作上結合されており、該プライバシーパラメータにしたがって該データベース表内のデータへのアクセスを制御する、データベース管理システムインターフェースとを含むことを特徴とするデータウェアハウス化兼管理兼プライバシー制御システムに存する。

【0012】第二の局面から見ると、本発明はデータウェアハウス化兼プライバシー制御システム内のデータソ

ースから得られるデータを管理する方法であって、データベース表内に格納されているデータに対するプライバシーパラメータの格納と取り出しを行うため該データベース表を拡張するステップにして、該データに関連する複数のデータベース表の列内に集合的に該プライバシーパラメータが格納されるステップと、該データベースからプライバシーパラメータを受信するステップと、該データに関連する列に該プライバシーパラメータを格納するステップと、個人プライバシーパラメータにしたがってデータベース管理システムインターフェースを介してのみ、該データベース表内のデータへのアクセスをリクエスト主体に与えるステップと、該データベース表へのアクセスをアクセスログ(access log)内に記録するステップとを含むことを特徴とする方法に存する。

【0013】別の局面から見ると、本発明はコンピュータで読むことができるプログラム格納デバイスであって、該コンピュータにより実行可能な一つ以上の命令を具備しておりデータウェアハウス化兼プライバシー制御システム内のデータを管理するための方法ステップを行うことができ、該方法ステップが、データベース表内に格納されているデータに対するプライバシーパラメータの格納と取り出しを行うため該データベース表を拡張するステップにして、該プライバシーパラメータが該データに関連する複数のデータベース表の列内に集合的に格納される、ステップと、該データベースからプライバシーパラメータを受信するステップと、該データに関連する列に該プライバシーパラメータを格納するステップと、個人プライバシーパラメータにしたがってデータベース管理システムインターフェースを介してのみ、リクエスト主体に対してリクエスト全体に対するデータベース表内データへのアクセスを与えるステップと、該データベース表へのアクセスをアクセスログ内に記録するステップとを含む方法であることを特徴とするプログラム格納デバイスに存する。

【0014】さらに別の局面から見ると、本発明はデータウェアハウス化兼管理兼プライバシー制御システムであって、複数の行および列にデータを格納する複数のデータベース表にデータを格納し、その表からデータを取り出すためのデータベース管理システムにして、該データベースに格納されているプライバシーパラメータにしたがって該データベース表内のデータが制御可能にアクセスできる、データベース管理システムと、プライバシーデータ登録と共に行うすべてのデータ、ユーザーおよびデータの使用を統括し(administering)、かつ該プライバシーパラメータにしたがって該データベース表内のデータへのアクセスを制御する、プライバシーメタデータシステムとを含むことを特徴とするデータウェアハウス化兼管理兼プライバシー制御システムに存する。

【0015】

【実施例】添付の図面のみを参照しつつ実施例を通して本発明を以下に説明する。

【0016】図1はデータウェアハウス化システム100の概観を表すシステムブロック図である。本システムは、中に一つ以上の拡張データベース(extended databases)106を格納するデータベース管理システム(database management system)104をもつ、保安データウェアハウス(secure data warehouse)102を含む。

【0017】データベースの一つの重要な能力は、仮想的な表(virtual table)を定義し、その定義をデータベース内にユーザーが定義した名称(ユーザー定義名称)と共にメタデータとして保存する能力である。このオペレーションにより形成されるオブジェクトはビュー(view)あるいはデータベースビュー(data view)として認識される。(以下、本発明で使用する特定のデータビューを「データビュー」と呼ぶ。)データビューは仮想的な表であるから、それが必要とされるまではデータベース内のどこにも物理的に顕在化されない。データへのすべてのアクセスは(管理上の目的で行われるデータアクセスは例外として)、データビューを介して達成される。種々のプライバシー規則(privacy rules、プライバシーを保護するための規則)を与えるため、一揃いの複数のデータビュー(以下、スイート(suite)という)が設けられる。プライバシーデータビューについてのメタデータ(データビュー名称、データビュー列の名称およびデータ型、並びに行を導出する方法を含む)はデータベースメタデータ内に持続的に格納される。しかしビューにより表される実際のデータはその導出された表と関連づけて物理的にどこにも格納されない。その代わり、データ自体が持続的なベース表(basetable)内に格納され、そのビューの行はそのベース表から導出される。データビューは仮想的な表であるが、ベース表に対してオペレーションを実行することができるのとまったく同様に、データビューに対してオペレーションを実行することができる。

【0018】保安データウェアハウス(secure data warehouse)102はさらに、拡張データベース106内のすべてのデータを表すプライバシーメタデータデータビュー(privacy metadata dataviews)108スイートを含む。データベース106内のデータはこのスイートのデータビューを通してのみ、閲覧、処理、変更をすることができる。拡張データベースおよびデータビューの方式および論理モデルをさらに詳しく図2との関連で述べる。

【0019】拡張データベース106内に格納されているデータへの実質上すべてのアクセスはデータビュースイート108を介してのみ与えられる。したがって、ビジネスアプリケーション110およびサードパーティア

アプリケーション112は、与えられたデータベースビューにより許可されるデータのみにアクセスできる。一実施例では、消費者のプライバシー・プリファレンス (preferences、好ましいものとして選択された事項) を無効にしようとする方が与えられる。しかし、そのような環境では、無効の原因がデータベースに記載され、それを監査モジュール (audit module) 118が取り出すことができる。したがって無効化が内幕に起きることはできない。さらに、無効化はプライバシー・メタデータ監視拡張機能 (privacy metadata monitoring extensions、以下PMD S拡張機能または単にメタデータ監視拡張機能という) 114によって監視することができ、無効化が起きるときは消費者に警告を与える。

【0020】データベースへのアクセスは、プライバシー・データ・ビュー・シート108により次の三つの目的の場合に制限して与えられる：(1) 個人データを匿名にするを可能にするためのプライバシー規則を用意すること、(2) 適用除外選択に基いて適用除外選択のために全行 (顧客レコード) を削除すること (これによって、取り扱っている顧客に対して何らかの有効な適用除外選択フラッグが設定されている行を削除し、したがってこれによっていかなる直接販売もサードパーティへの公開も阻止する)。

【0021】データビュー108と通信するクライアント・インターフェース・モジュール122を使用して、クライアント124はクライアント124から収集されたデータにアクセスし、制御し、管理することができる。このデータの制御および管理は、(適当なブラウザプラグイン128、モデム130、音声による電話通信機132あるいはキオスク134、POSにあるその他のデバイスを介する) インターネット126を含む広範囲の通信媒体140を使用して、達成することができる。そのような通信を助けるため、キオスクやPOS (販売点) にあるその他のデバイスはスマートカード136あるいは愛顧者カード138を発行することができる。キオスク/POS装置134はプライバシー・プリファレンスに関する消費者入力を受信し、これらのプリファレンス値に関する情報を格納したスマートカード136あるいは愛顧者カード138を発行することができる。同様に、キオスク/POS134、スマートカード136、あるいは愛顧者カード138を使用して、消費者は必要に応じてプリファレンス値を更新し、あるいは変更することができる。愛顧者カード138が単純な読取り専用装置 (キー・リングに装着されたバーコード装置等) である場合は、キオスク134は必要に応じて情報を更新した取り替えカードを発行することができる。愛顧者カード138あるいはスマートカード136を使用する取

引は選択的に暗号化し、匿名にすることができる。いずれのカードも選択した保安規則を与えるべく、直接あるいはプラグインを介してサーバと対話することができる。

【0022】このインターフェースを介して消費者はデータ・シェアリング (data sharing) および保持 (retention) のプリファレンスを指定することができる。これらのプリファレンスにはデータ保持プリファレンスおよびデータ・シェアリングプリファレンスが含まれる。これらのプリファレンスによって、消費者はいついかなる状況の下で個人情報を保持し、または共有しあるいは他人に販売しうるかを指定することができる。例えば、当該消費者はそのようなデータを愛顧者カードプログラムの一部として保持することができ、あるいはそのデータの使用を特定の使用に限定することができる。さらに、消費者はいついかなる状況の下でそのデータが即時販売され、統計的解析の目的に使用され、あるいはサードパーティの選択的マーケティングプログラムの目的に使用されるかを指定できる。

【0023】データ・データウェアハウス化システム100はまた、プライバシー・サービス150を介してクライアントと保安データウェアハウス102との間の匿名通信を可能にする。ユーザーが匿名の取引を望むときは取引はプライバシー・サービス150へ送信される。プライバシー・サービス150はプライバシー規則データベース152および他の保安情報154にアクセスし、プライバシー規則および保安情報を使用して消費者の身元を決定できるすべての情報を除去 (浄化) する。浄化された取引情報は次いで保安データウェアハウス内の匿名保護インターフェース・モジュール160へ回送される。保安データウェアハウス102との通信はプロキシ・ユーザー・同定手順を使用する。この同定はプライバシー・サービス150により消費者の使用名または他の同定情報から生成される。もしも顧客が匿名取引を必要としないなら、取引は、拡張データベース内に取引情報を格納できる小売業者に直接に提供される。

【0024】データ・ビュー・シート108は単独に拡張データベース内のデータへのアクセスを与えるので、データ・ビュー・シート108もまた保安データウェアハウス102の保安を監査するための便利かつ合理的な手段を与える。

【0025】保安データウェアハウス102もまたメタデータ監視拡張機能114を含む。このメタデータ監視拡張機能114によって顧客は個人データの使用を監視するための規則を発生させることができ、またメタデータ定義の変更が生じたときは警告116または取り消しを送信することができる。顧客の個人情報が拡張データベース106から読み取られるとき、または拡張データベース106に書き込みがなされるとき、拡張データベース106に格納されている適用除外選択リミット (opt-

out delimiters) が変更されるとき、あるいは表またはデータビューがアクセスされるときに、消費者はメタデータ監視拡張機能 114 を制御して警告を発生させることができる。この代わりに、顧客が後でアクセスできるよう、発生した警告を記録しておくことができる。

【0026】メタデータ監視拡張機能 114 はまたデータソース情報を記録するので、顧客は保安データウェアハウス 102 に格納されているデータのソースを決定することができる。データソースは顧客であるかも知れない、あるいはサードパーティを媒介とするソースであるかも知れない。本発明のこの特徴は、顧客が誤った情報を訂正したいときのみならず、当該誤りが同じデータベースもしくは他のデータベースで繰り返されることがないように、誤った情報ソースを特定したいとき、特に有用である。

【0027】またデータのソースを直接に表データから確認することができるよう、ソースデータはデータ表の各列とあるいは一組の列に格納することもできる。本実施例では、メタデータ内に情報ソースの情報をすべての顧客に対して複製するをなくとも各顧客が異なる情報ソースをもつことができるよう、ソースを同定するデータを一般化することができる。

【0028】同様にまたメタデータ監視拡張機能 114 も、データターゲット情報を記録するので、顧客は誰が彼らの個人情報の受信者であるかを決定することができる。この特徴もまた顧客の個人情報に関して公開活動を監視する上で有用であるのみならず、複製された誤りを訂正する上で、有用である。

【0029】メタデータ監視拡張機能 114 はまた、プライバシーデータビューシート 108 への変更のみならず拡張データベース 106 からの読み取りおよびそれへの書き込みを追跡することにより、監視機能のサポートに使用することができる。

【0030】本発明は、プロセッサおよびランダムアクセスメモリ (RAM) のようなメモリを含むコンピュータに実現することができる。そのようなコンピュータは普通、ディスプレイと動作上結合しうる。ディスプレイは、ユーザー向けウィンドウのようなイメージをグラフィックユーザーインターフェース上に表示する。コンピュータはキーボード、マウス装置、プリンタ等の他の装置に結合することができる。もちろん、当業者は上記のコンポーネントの任意の組合せあるいは任意数の異種コンポーネント、周辺機器その他の装置をコンピュータに使用することができることを認識できよう。

【0031】一般に、コンピュータはメモリ内に格納されているオペレーティングシステム、およびユーザーインターフェースの制御のために動作する。ユーザーインターフェースは入力およびコマンドを受信すると共にグラフィックユーザーインターフェース (GUI) モジュールを介して結果を表示する。GUI モジュールは普

通、別個のモジュールであるが、GUI 機能を実行する命令はオペレーティングシステムまたはアプリケーションプログラム内に常駐させ、分布させ、あるいは特別の目的のメモリおよびプロセッサを使って用意することができる。コンピュータはまた、COBOL、C++、FORTRAN その他の他のプログラム言語で書かれたアプリケーションプログラムがプロセッサで読み取りできるコードに翻訳しうるコンパイラをもつことができる。翻訳完了後、アプリケーションは、コンパイラを使って発生された諸関係式および論理を使用してコンピュータメモリ内に格納されているデータにアクセスし、操作する。

【0032】本実施例では、オペレーティングシステムをなす諸々の命令、コンピュータプログラムおよびコンパイラはコンピュータが読み取り可能な媒体、すなわちデータ格納装置 170 内に実体的に実現される。この格納装置 170 はジップドライブ、フロッピーディスク、ハードウェアドライブ、CD-ROM ドライブ、テープドライブ等の一つ以上の固定式もしくは着脱式データ格納装置でよい。さらに、オペレーティングシステムおよびコンピュータプログラムは諸々の命令からなるが、これらの命令は、コンピュータにより読み取られて実行されると本発明を実現およびまたは使用するのに必要な諸ステップをコンピュータに行わせるものである。コンピュータプログラムおよびまたは諸々の命令もメモリおよびまたはデータ通信デバイス内に実体的に実現することができる。それにより本発明に基づくコンピュータプログラム製品あるいは製造物品を作製することができる。上記のとおりであるから、「プログラム格納装置」、「製造物品」および「コンピュータプログラム製品」と言う用語はここではコンピュータにより読み取り可能な任意の装置、あるいは媒体からアクセス可能なコンピュータプログラムを含む。

【0033】当業者は、本発明の範囲から逸脱することなくこの形態に任意の変更を加えることができることを認識されたい。例えば本発明は上記のコンポーネントの任意の組合せ、あるいは任意数の異なるコンポーネント、周辺機器その他の装置を本発明に使用することができることを認識されたい。

【0034】論理モデル

図 2 は保安データウェアハウス 102 およびデータビューシート 108 の論理モデル例をより詳細に示す図である。拡張データベース 106 は表 202 を含んでおり、この表は次の三つの部分：同定情報部分 204、個人情報部分 206、および機器情報部分 208 に分割される。個人情報部分 206 はデータ列 220、232、244、および 246 を含む。これらの列は消費者の身元を表す情報を格納する。これらの列には消費者口座番号列 220、氏名列 232、住所列 244、および電話番号列 246 が含まれる。顧客表 202 の同定部分 20

4も一つ以上のデータ制御列212を含んでおり、これらの列はプライバシープレファレンスをなす表中の関連データに対する「適用除外選択」を反映するデータを特定している。ここに例示した実施例では、列222-230は一つ以上の文字「A」または「D」すなわち当該顧客のデータコードに対するプライバシープレファレンスを指定するフラッグ（「1」および「0」で表されている）を格納する。ここに開示する実施例ではこれらのプライバシープレファレンスは次の事項に対する「適用除外選択」を含む：（1）直接販売、（2）当該顧客を特定する情報および個人データの公開、（3）匿名による個人データの公開、（4）自動マーケティングの判定を行うための個人データの公開、および（5）機密データの公開と使用。表202はまた、グローバルデータ制御列210を含む。この列は顧客が最大限のプライバシーを望むことを示すのに使用することができる。

【0035】ここに例示する実施例では、「ビル K ジョーンズ」という名前の顧客がグローバルデータ制御列210に「0」を選択することにより、ある程度のデータ収集、解析、あるいは流布を許可している。彼はさらに、彼の身元情報と共にあるいは匿名で、彼の消費者情報を直接販売に使用することができること、およびサードパーティに公開できることを示している。彼は自動処理を行うのにデータを使用することを許可しているので、機密データを流布することを許可するであろう。

【0036】一実施例では前述の論理モデルを実現するのにテラデータ（TERADATA）データベース管理システムが使用される。これを使用することにはいくつかの利点がある。

【0037】第一に大量のデータを格納し取り扱えるテラデータの能力が多数のいろいろのビューの構築を容易にするとともに、保安データウェアハウス化システム100が論理データモデルを第三の正規の形態でもしくは正規の形態に近い形で利用することを可能にする。

【0038】第二に、データビューサブセットまでデータを狭めるための一連の選択としてSQL照会（SQL queries）を実行するシステムとは異なって、本テラデータデータベース管理システムは適当なベース表から直接に必要な列を選択するSQLを発生すべくデータビューベース（dataview base）の照会を書き直す。他のビューはデータをビューサブセットにまで狭める前に表全体を作成するが、テラデータは適当な列および行の結果表（処理結果をまとめた表）中に選択的に引き抜くSQLを発生する。この方法は、前述の論理モデルを実現するのに特に有利である。

【0039】第三に前述の論理モデルは一般に複雑な照会および広範なSQLステートメントを含むデータビューを生ずる。テラデータデータベース管理システムは、そのような照会およびSQLステートメントを最適化す

るのに特に有効である。

【0040】上に教示したことを使用して、特別な個々のプライバシー条件に合うよう、かつ各データベースアプリケーションを制御するのに必要な条件に合うよう、代わりの定義データ制御列構造を有する代わりの論理モデルを実現することができ。

【0041】データビュー
データビュースイート108には多数のデータビューが用意されている。これらのデータビューには標準ビュー260、特権ビュー（privileged view）262、匿名ビュー（anonimizing view）264、および適用除外選択ビュー266が含まれる。これらのビューはデータ制御列212に置かれている値に基づいて顧客表202内のデータへの可視度（visibility）を制限する。

【0042】標準ビュー260は、列224内のフラッグ（個人情報および同意情報）が流布できることを意味する）あるいは列226（個人情報匿名でのみ流布し得ることを示す）のいずれかがアクティブ化されない限り、個人データを表示しない。したがって、標準ビュー260は消費者が適当なフラッグを適当な値に設定しない限り、個人データを選択的にビューから隠す。

【0043】スケラブルデータウェアハウス（scalable data warehouse, SDW）の顧客データベース統括者（customer database administrators）は、ルーチンユーザーに対しては個人情報のすべての列が隠されるように、顧客表（顧客に関する個人情報を含む任意の表）の中に入るビューを設定する。これにより、すべてのルーチン決定サポート（routine decision support, DSS）アプリケーションおよびウェアハウスデータへの照会アクセスを備えたツールを個人情報の閲覧から適用除外することができる。その結果これらのアプリケーションおよびツールのすべてのエンドユーザーも同様に個人情報の閲覧から適用除外される。

【0044】既存のSDW顧客に対して混乱が生じるところを最小限に留めるため、プライバシーデータにアクセスする既存のすべてのアプリケーション内のベース表に使用されるものと同一の氏名を使用してデータビューが設立され、その氏名に対応するベース表の氏名が他の値に命名し直すことができる。こうして、既存アプリケーションが（ここではデータビュー経由で）私的データへアクセスしようと試みても、その私的データはユーザーがもつ特権に依りてデータビューによりふりふり隠され、このアプローチを使用すれば既存のアプリケーションを変更する必要はまったくない。その代わり、論理データモデルおよびデータベースの方式が変更され、更なる命名規約が導入される。

【0045】特権ビュー262は、データベースの管理およびまたは維持（例えば新規顧客の挿入、前顧客の削除、住所変更など）に必要とされる特権的（クラス「A」の）アプリケーション108に対してのみ、お

およびプライバシー関連機能（顧客について収集された個人情報に顧客に通知すること、個人情報を変更/更新すること、および「適用選択/適用除外選択」制御を適用することなど）の関連機能）を取り扱うアプリケーションに対してのみ、提供される。例えば、顧客プライバシーフェレンスを閲覧し、指定し、変更するのに使われるクライアントインターフェースモジュール122は、特権アプリケーションである。特権アプリケーションは特権アプリケーションであると適切に同定されることを確実にしめると共に、特権ビュー262が承認されていない任意の主体によるアクセスを防止するため、適当な保安対策がとられる。

【0046】ある種のSDWアプリケーション（「クラスB」）は顧客の振る舞いの見通しを得るため、例えば顧客の傾向あるいは行動パターンを同定するため、個人データに解析を施すことができる。そのようなアプリケーションは（知的業務者あるいは「パワーアナリスト」と呼ばれる）エンドユーザーが駆動することができる。かかるエンドユーザーとは典型的に照会を行うことができるエンドユーザー、典型的にはカスタム構築したソフトウェアあるいは標準的照会もしくはOLAPツールを使って、上記のパターンを発見するようなエンドユーザーである。彼らエンドユーザーは発掘ツール（data mining tools）も使用することができる。このツールでは統計的もしくは機械学習アルゴリズム（machine learning algorithms）が当該アナリストと共にパターンを発見し、そのパターンからアナリストが予測モデルを構築する。

【0047】最も有効な値を導出するため、解析アプリケーションは利用可能なすべての形態の個人情報にアクセスしなければならない。必要とされる個人のプライバシーを尊重すると同時にそのようなアクセスを可能にするため、特別の「匿名化」データビューが使用される。これらデータビューは個人データフィールドへのアクセスを提供するように設計されているが、データ所有者を同定できる情報（例えば氏名、住所、電話番号、社会保障番号、口座番号など）を含むすべてのフィールドを遮蔽するように設計されている。

【0048】匿名化ビュー264は個人情報の閲覧および解析を許すが、列224内のフラッグ（当該消費者を同定する情報と個人データの公開を許可するフラッグ）が選択されていない限り、同定情報部分204に格納されている情報を閲覧および解析から遮蔽する。このデータは解析アプリケーション110Cに提供することができる。このアプリケーションはデータ発掘および典型的照会を許容する。消費者が許可するなら、この情報はまたサードパーティアプリケーション112にも与えることができる。

【0049】別のクラスの特権アプリケーション（「クラスC」）にはある形態の処置（action）を行うために

個人情報を使用するアプリケーション、たとえばマーケティングアプリケーション（郵便もしくは電話による勧誘を行うものなど）が含まれる。これらのマーケティングアプリケーションは各顧客に対して設定された「適用選択/適用除外選択」制御を受け、アクティブ化された「適用除外選択」指標（indicator）をもつすべての記録を除去しあるいは隠す特別のデータビューを介して、顧客情報にアクセスする。したがって、例えばマーケティング勧誘を受信しない選択をした任意の顧客は、マーケティングアプリケーションが生成する任意の接触リストから適用除外される。

【0050】「適用除外選択」指標はデータビュー経由で顧客表に追加され、あるいは既存の顧客表に接合される新規の列である。（これは論理データモデルに追加される変更である。）一実施例では、各顧客行に対するこの列の値は、初めは「適用除外選択」に設定される（あるいは法律で許可されるなら「適用選択」に設定される）が、クライアントインターフェースモジュール122経由で改変することができる。このモジュール122はプライバシー制御に関する顧客のリクエストを処理する。

【0051】多重「適用除外選択」指標は、各顧客レコードに対して設定することができる。最小限、「直接販売」、「身元データのサードパーティへの公開」、「サードパーティへの匿名データの公開」、「自動判定」、および「機密データの使用」に対する5個の適用除外選択が用意される。しかし、さらに詳細な顧客のプレファランスに基づいてさらに詳細に分類した適用除外選択を設計することができる。例えば、「直接販売」に対する適用除外選択項目は、電話、ダイレクトメール、および電子メールによる接触、および「その他」の処置のための複雑事項に分けることができる。こうすると8個の別個の適用除外選択が生じる。

【0052】適用除外選択ビュー266は処置アプリケーション110Dによって自動判定（automated decisions）を行うために情報を利用することは許可する。そのようなアプリケーションはたとえば電話あるいは郵便による勧誘などの処置を行うものである。この情報閲覧は列228内のフラッグにより制御される。列228に格納されている値は、この代わりとして十分な値域をもつ一文字を含むことができる。その文字は、当該勧誘が許可されることを定義するに留まらずいかなる種類および範囲の勧誘が許可されるかを指示することを許容できる。

【0053】（マーケティングや解析等を目的として）サードパーティに個人データを公開しあるいは照会するアプリケーションはクラスC（「適用除外選択」）のビューおよびクラスB（「匿名」）のビューの両方を受ける。もしも顧客が、サードパーティによる自分のデータの使用を適用除外とする選択をしていると、「適用除外

選択」データビューが適用され、それらの行(レコード)は出力から適用除外される。他の顧客は彼らのデータが匿名であることを条件にサードパーティへの公開を「適用選択」しているかも知れない。そのような場合には顧客データは出力される前に「匿名化」データビューを介して匿名化される。他のすべての場合は顧客は身元が特定できる形式で自分の個人データが公開されることの適用選択をしている。この場合は個人データが身元同定データと共に出力される。

【0054】適用選択もしくは適用除外選択をするためのさらに細かい分類を用意することができる。種々の許可および保護に関して顧客毎に同意を求め、特定の適用選択もしくは適用除外選択を設定できる。例えば、サードパーティへの公開は、個人の特徴および個人の身元の両方に関連する特定のデータに基づいて行うことができる。顧客は自分の住所および関心事項のプロファイルを提供することに同意するが、経済情報および電話番号については同意しないこともあり得る。

【0055】適用選択/適用除外選択は各顧客のさらに詳細なプロフィールおよび関心事が得られるようにさらに拡張することができる。例えば、適用除外選択(例えば第4節で同定した8個の適用除外選択)のクラスをそれぞれ別個に各範疇の個人データ(例えば人口統計学的データ、プロフィールデータなど)に適用することができようし、あるいは個人データの各特定データ項目(例えば年齢、性別、ハイキングの趣味、好みの靴ブランドなど)にまで適用することができる。このようにして、顧客はいくつかの関心領域に関連するいくつかの処置を適用除外選択することができ、他の項目を適用選択する(例えばランニングシューズについてダイレクトメールの受信を適用する)ことができる。

【0056】図3はさらに細かく分類された適用選択および適用除外選択を備えた保安データウェアハウス102の、別の論理モデルを示す。この実施例では、各クラスのプライバシープレファレンスが各範疇のデータ(例えば人口統計など)に別個に適用され、あるいは個人データ(例えば年齢、性別、ハイキングの趣味、あるいは好みの靴ブランド)の各特定データ項目にまで適用される。例えば、消費者ビル・K・ジョーンズはいくつかの目的には彼の氏名へのアクセス許可するが、その他の目的にはアクセス不可とする選択をなしている。これらの制限は列302-310の記入事項として適切な組合せのフラッグを入力することにより選択することができる。同様にジョーンズ氏の名前の格納およびまたは使用に關してプライバシープレファレンスを指定するのに列312-320を使用することができる。列312-320に定義されたプレファレンスは、列302-310に記録されたものと異なるかも知れないし、同一かも知れない。本発明はまた、さらに詳細な顧客のプレファレンスに基づいて、前述の保安プレファレンス範例(secure

preference paradigm)を細密な多重的プレファレンス(multiple fine-grain preferences)へ拡張することを実現する。例えば、直接販売は電話、ダイレクトメール、電子メール、および「その他」の処置をとりたいキャッチコールに対する別々のプライバシープレファレンスに分解することができる。さらに、直接販売の範囲を一回の接触だけを許可するように指定することができる。

【0057】別の実施例ではデータ暗号を使用することによって、拡張データベース106およびデータビュースイート108が果たす特徴的な保安およびプライバシー保護がさらに強化される。これは与えられたデータのデータを暗号化コードで暗号化することにより、あるいは各データフィールドに固有の暗号化数を与えることにより、行うことができる。その代わりとして、消費者のプライバシープレファレンスを実行することができるようにいろいろの階層的レベルでデータを暗号化することもできる。

【0058】一実施例では暗号化技術は任意の同定フィールド上で使用されたと共に行単位でも選択的に適用される。この技術によれば、顧客が(例えばデータを発送する目的などで)匿名のままに留まることを可能にする一方、データ暗号化権を有するアプリケーションもしくはデータ請求者に対しては積極的に身元の同定を受け入れることが可能になる。

【0059】データビューのオペレーション
本発明のデータベーススイート108におけるデータビューは、ベース表の適当な列および行を結果表中に選択的に引き入れるSQLステートメントを発生する。(データをビューサブセットにまで狭める前に表全体を作成する)従来技術と比較して、本技術はデータ請求者にデータを表示するために必要な処理を低減する。

【0060】データベース所有者すなわちBBB ONLINE、TRUSTE、PRICE-WATERHOUSE、TRW、DMAあるいはCPA WEBTRUST、あるいはNCRのような独立の監査サービスは、定期的にもしくは苦情を受けたときに、安価にデータベースの見直し(review)を行うことができる。これらの見直しでは論理データモデルとデータベースのスキーム、当該システムを使用するアプリケーションとユーザー、およびデータアクセスログが調査される。

【0061】論理データモデルの見直しでは、データビュー構造を調査し、(個人情報へのアクセスを制限している)正規ユーザー用の「標準」ビュー、解析アプリケーション用の「匿名」ビュー、およびその他のアプリケーション用の「適用除外選択」ビューの存在が調査される。

【0062】これらのアプリケーションの見直しおよびユーザーの見直しは、アプリケーション、ユーザー、およびそれらに付与されているアクセス権を調査する。こ

の見直しは、「クラスA」特権をもつアプリケーション／ユーザーが「個人データ」データビューへのアクセス権をもっていること、「クラスB」解析アプリケーション／ユーザーが「匿名化」データビューへのアクセス権をもっていること、「クラスC」処置アプリケーション／ユーザーが「適用除外選択」ビューへのアクセス権をもっていること、個人データの出力表あるいはファイルを生成するアプリケーションが「適用除外選択」および「匿名化」ビューへのアクセス権をもっていること、並びに他のアプリケーションが「標準」ビューを使用することの確認を行う。

【0063】最後に、テラデータアクセスログあるいは別のデータベース管理システムから得た類似のログが見直される。これは行われたアクセス活動が当該データベースにより規定されているプライバシーパラメーターに適合していることを確認するためである。

【0064】図4は本発明の特徴であるプライバシー監査オペレーションの概観を表す図である。データ請求主体が拡張データベース106内のデータへのアクセスを望むときはいづれも、リクエストはデータベース管理システムインターフェース109に対してなされ、インターフェース109がプライバシーパラメーターにしたがって当該データベース内のデータのアクセスを制御する。当該リクエスト主体のステータスに基づいてデータビューシート108からリクエスト主体に与えられるデータビューを使って、拡張データベース106の表がアクセスされ、そのデータが提供される。同時に、データベースアクセス（アクセスが不成功であるときはその試みられたアクセス）がアクセスログ（access log）402に記録される。アクセスログ402は、アクセスもしくはアクセスの試みの形態、アクセスを生じたリクエストのテキスト（SQL）、アクセスの頻度、リクエストされた処理、リクエスト主体またはアプリケーション名または識別データ、および参照されたオブジェクト（表、データビューおよびまたはマクロ）に関する情報を含む。アクセスログ402により、データビューシート108内のデータビュー、マクロシート111内のマクロ、あるいはデータベース106内のベース表へのすべてのアクセスを監査することができ、アクセス権を付与しまたは呼び出す総ての活動が同様に監査できる。これが可能であるのは、アクセスログ402の内容と表／データビュー／マクロの定義とからプライバシー規則が施行されているかあるいは破られているか決定ができるからである。

【0065】プライバシー監査モジュール118が設けられるのは、プライバシーパラメーターを有効に適用するべくアクセスログ402内のデータについてプライバシー解析を行うためである。プライバシー監査モジュール118はプライバシーに関するすべてのイベント（even t）を追跡し、個人データへのアクセスに関する活動を

要約し、プライバシー規則のいかなる疑惑ある違反にもフラッグを立てる。プライバシーテストスイート404は、プライバシー規則を「破る」ことを試みてからアクセスログ402を調査してプライバシー規則が適用されたかあるいは破られたかを決定するプログラムその他の手順を含んでいる。プライバシー監査モジュール118はこれを、顧客プライバシープレファレンスが適用されているかを独立に評価するサービス監査者またはデータウェアハウスマネージャが使用できるように、手直しできる。

【0066】メタデータサービス

メタデータサービスはプライバシーメタデータサブシステム（privacy metadata subsystem, PMS）拡張機能114を含む。PMS拡張機能114は多数のパラメーターを格納し、追跡するとともにこれらのパラメーターを使ってプライバシーが関わる活動を追跡する。追跡されたパラメーターには、（1）システムに現在あるすべてのデータエレメント（データベース、ユーザー、表、ビューおよびマクロを含む）のデータ復号化、（2）システムに対してソースとなった内部エレメントのデータ復号化、（3）システムに対してソースとなった外部エレメントのデータ復号化、（4）システムにとってターゲットとなった内部エレメントのデータ復号化、（5）システムからアクセスポートされたデータエレメントのデータ復号化、（6）すべてのユーザー、グループおよびアプリケーション並びに当該データへのそれらのアクセス権のプロファイル、（7）データのアクセス／更新、表／ビュー／マクロの生成、特権の付与／取消し、ユーザープロファイルの変更、およびトリガーに関するイベント記録を含む。

【0067】PMS拡張機能114はまた、プライバシーに固執するデータコントロールを支配する実行可能なビジネス規則と、テラデータログ（例え記録の開始／終了）の操作（manipulations）に関するイベントの記録もしくは別のデータベース管理システムにおけるそれと類似の記録に関するイベントの記録とを格納し管理する。

【0068】また、PMS拡張機能114はプライバシーが関わるメタデータを見直し、管理するための高レベルGUI406をプライバシー統括者に提供する。このGUIは、すべての顧客（消費者またはデータの主体）の情報に対するデータベースとそれらの表／ビューマクロ構造のグラフィック表示、および関連するユーザー／ユーザーグループの特権のグラフィック表示を含む。またGUI406は、プライバシー統括者がGUI406を介して与える定義に基づき、プライバシー規則を設定すると共にその設定の結果、データビュー、マクロ、もしくはアクセス権を発生するパラメーター駆動手段（parameter-driven means）を提供する。またGUI406は、外部監査者が当該サイトのプライバシー保護

策の見直しを行う際に彼を案内する便宜を提供する。

【0069】PMD S拡張機能114はまた、報告を行う便宜の機能を提供する。これは種々のデータベースおよびPMD Sログの内容を解析してプライバシー関連の活動に関して報告を行うものである。プライバシー統括者はそのようなプライバシー報告を対話型インターフェースもしくは印刷された報告を介して見直すことができる。独立の監査者はプライバシー統括者と共に、そのような報告の助けを借りて監査を行うことができる。

【0070】またPMD S拡張機能114は、消費者の個人データおよびそれに関連するプライバシー規則へのアクセス、それらの見直し、および訂正を行う消費者をサポートするためのGUIアプリケーション/ユーティリティを別途提供する。またPMD S拡張機能114は、プライバシー関連のイベントに関するさらに詳細な記録をとるための便宜を提供することもできる。

【0071】マクロ

単独であるいはここに記載するデータビューと組み合わせてマクロ111（すなわちデータベース管理システムインターフェースに格納された手順）を使用してデータの制御とデータへのアクセスを記録することができる。データプライバシーパラメーターを適用するべくマクロを使用する場合は、ユーザーは「選択」アクセス権を与えられない。その代わり、ユーザーは、マクロスイート111内のマクロへのアクセス権を与えられる。このマクロは実際のデータアクセスを行うと共に将来の監査を目的としてアクセスログ402内のイベントを記録する。その場合も、これらのマクロは適用除外選択された行および列へのアクセスを制限する前記ビューを通して当該データに対して実行される。そのようなマクロは単一行アクセスを記録するのに特に適している。

【0072】データ辞典

データ辞典408は、システム内のすべての表、データビュー、およびマクロ、システム内のすべてのマクロ、すべてのユーザーおよび彼らの特徴（ユーザーが所有しているマクロに関する特権を含む）を含めたデータベーススキーマに関する情報を格納している。

【0073】プロセス

図5は本発明の一実施例を実行するのに使用されるオペレーション例を示す流れ図である。このプロセスはブロック502に示すように、表のデータに関連をもつ以上の列にプライバシープレファレンスを格納し、それを取り出すため、データベース表を拡張することにより始まる。この拡張されたデータベース106は、データ（個人的および非個人的データ）およびプライバシーパラメーターを格納するための論理モデルを形成する。普通、このデータベースは初期、プライバシーを最大に保護するべく選択されたプライバシーパラメーターが多数入れている（すべてのデータの収集、解析および配布を適用除外する選択がしてある）。事件が許すときは、初期

データベースはより低度の、ときには最小限の、プライバシー保護を選択するプライバシーパラメーターで多くすることもできる。

【0074】次にブロック504に示すようにデータベースからプライバシーパラメーターを受信することができる。この意味では通常、そのデータベースはデータの究極的なソース（消費者）である。しかし他の実施例では、データベースは、データをどのように使用するか、もしくは共有するかに関する命令を含んだデータを与えている、媒介者たるサードパーティであり得る。その場合、これらの命令は、これらの命令に基づいてそのデータが使用されもしくは配布されることを保証しなければならない。

【0075】ブロック504に示すオペレーションはクライアントインターフェースモジュール122とコンピュータのようなクライアントの通信装置とを介して達成することができる。かかるコンピュータはインターネットブラウザ128（ブラウザプラグインを備えたものなど）および電話接続線と備えた簡単なモデム130を走らせているものでよい。このオペレーションは、電話132を介して（実際のあるいはコンピュータ上に用意された）サービス担当者に話すことにより、またはキオスクもしくは自動現金預け払い機（ATM）134を通して、またはデータベースプレファレンスを受信しそれをクライアントインターフェースモジュール122へ送信できるその他の装置を通して、行うことができる。これらのいずれの場合でも、データベースは個人データを閲覧すること、およびデータベースの必要条件に合致するプライバシーパラメーターを選択することができる。インターネットブラウザ128、モデム130、キオスクもしくはATM134を通してアクセスが与えられる場合は、上記装置に用意されているプライバシーウィザードを使用することにより、本プロセスの過程でユーザーを案内することができる。データソースは、愛読者プログラムをもらう交換条件としてデータの収集、解析、あるいは配布の活動のいくつかを適用を受け、との選択ができる。一旦データソースのプライバシーパラメーターが得られると、それらのパラメーターはプライバシーパラメーターの主体のデータに関連する列内に格納される。これはブロック506に示してある。リクエストをしている主体がデータへのアクセスをリクエストすると、データベーススイート108、マクロスイート111、あるいはその両方を経由してデータベース管理システムインターフェース109を通してのみアクセスが与えられる。したがってデータは確実にデータソースの個人プライバシーパラメーターにしたがって与えられる。

【0076】図6は、データベース管理システムインターフェースを通してアクセスを与えるために使用するオペレーション例を示す流れ図である。第一に、ブロック

602に示すように、リクエスト中の主体からデータリクエストが受信される。次に照合確認されたリクエスト主体の身元にしたがって選択されたデータビューが与えられる。リクエスト主体はこのデータビューを使用してデータベースにアクセスし、データを得ることができる。一実施例ではデータビューは前もってリクエスト主体に与えられ、リクエスト主体は所望するデータにアクセスするためにのみそれらを使用することができる。もう一つの実施例ではデータビューはデータリクエストに呼応してリクエスト主体に与えられるが、データビューはそのデータリクエスト、当該データに関連したプライバシーパラメータ、およびリクエスト主体の身元にしたがって手直しされる。

【0077】図7は本発明の一実施例においてプロキシサービスリクエスト(proxy service request)を受信するために使用するオペレーション例を示す流れ図である。この実施例はクライアント(または消費者)に小売業者その他の主体と匿名の取引を行う能力を与える。これはプライバシープロキシサービスを使って達成される。このプライバシープロキシサービスは消費者と小売業者(またはデータベース管理システム)との間の匿名化インタプリタ(anonymizing interpreter)を与える。プロキシサービスリクエストが(将来のデータソースたる)プライバシープロキシサービス150内のクライアントから受信され、受容されると(ステップ702)、そのクライアントに対するプロキシの識別データが取り出される。もしもそのクライアントに対するプロキシ識別データが存在しないと、将来の使用に供するためのプロキシ識別データが発生され、クライアントに与えられる。これらの取引はインターネットブラウザプラグイン128、モデム130、あるいはキオスク/ATM134を通して行うことができる。クライアントは、小売業者ごとに、あるいは個人情報収集することができる他の主体ごとに、異なる匿名化プロキシ識別データをもつことができる。その場合、クライアントのプロキシ識別データ管理を援助するための手段が与えられる。これはクライアントのスマートカード136上にデータの格納と処理を行うこと、要顧客カード138にデータを格納すること、およびまたはキオスク/ATMあるいは販売点(POS)134において追加的処理を行うことにより、達成することができる。

【0078】図8はデータソースからアクセスリクエストメッセージを受信するために使用するオペレーション例を示す流れ図である。本発明はまた、クライアント(あるいはデータソース)が特権ビュー262を使って個人データにアクセスし、データの収集、格納、および流布を制御することを可能にする。第一に、ブロック802に示すように、アクセスリクエストメッセージがクライアントから受信される。次にブロック804に示すように特権データビュー262がクライアントに与えら

れる。特権データビュー262はクライアントの個人プライバシーパラメータへのアクセスを与えたとともに、クライアントがこれらのプレファレンスを閲覧し、変更することを許す。

【0079】代わりの実施例

図9は本発明の代わりの実施例を示すブロック図である。この実施例では、二つのデータベースが使用される。その最初の名は匿名化されたデータベース908で、これは表906の中に格納されているデータに関連した匿名化されたデータとと筆名(pseudonyms)とを格納する。第二のデータベースは、信託データベース(trusted database)904で、筆名を顧客認識情報に関連づける表902を格納している。この実施例では顧客の氏名は信託データベース904に別個に格納されている。このデータベースはこれをデータ管理システムインターフェース109が使用して、顧客の身元を筆名に、したがって匿名化されたデータベース908内に格納されているデータに、結びつける。信託データベースは個々人のプライバシーパラメータをも格納している。

【0080】クライアントの筆名は、要顧客カード138もしくはスマートカード136を発行することによって、またはインターネット126もしくはクライアントコンピュータとのオンライン通信により、またはその他の手段により、クライアントに提供される。次いで筆名は消費者の取引に対するプロキシとして使用することができる(したがって収集された任意のデータを匿名のままに保持することができる)。顧客の身元同定のためのデータ発露を防止するため、必要であれば異なる業者または異なる店舗に対して異なる筆名を使用することができる。

【0081】顧客は非匿名データの収集、使用、あるいは流布を許可するようにデータプライバシープレファレンスを選択することができる。これらのプレファレンスはデータ管理システムインターフェース109により適用され、クライアントにより要顧客カード138、スマートカード138、インターネット126、およびその他の通信/データ格納方法を使用して提供される。一実施例ではインテリジェントソフトウェア エージェントがデータ発露機能を実行して顧客の行動パターンを調査すると共に、発露した結果に基づいてデータプライバシーパラメータを提案する。

【0082】別の実施例では、多重レベル保安プライバシーシステムにおいて別個の信託データベース904および匿名データベース908を使用する。この場合は異なる法制によるプライバシー保護の条件やいろいろな小売りアウトレットに適合し、またはいろいろの個人プレファレンスを許容するため、ここに開示した暗号化の方法、マクロ、データビューおよびまたは別個のデータベース技術を組み合わせる。

【0083】図10はプライバシーデータウェアハウス

の別の実施例を示す図である。前述した実施例におけると同様、データベース管理システム104のデータへのアクセスは、再びデータベース108内のデータビューを介して、あるいはマクロスイート111内のマクロ2を介して達成される。この実施例ではプライバシーサービス150、クライアントインターフェースモジュール122、メタデータ監視拡張機能114、および監査インターフェース118を含むプライバシーメタデータサービスインターフェース102もデータベース管理システム104への全アクセスの途中に配置される。プライバシーメタデータサービスインターフェース102はそれゆえ、データベース管理システム104、データビュースイート108内のデータビュー、およびマクロスイート111内のマクロへのすべてのアクセスを制御することができる。

【0084】図11はプライバシーメタデータサービスインターフェースが介在するデータビューの実施例を示す図である。データベース管理システム104の顧客ベース表内のデータの可視性およびデータへのアクセスはデータビューおよびマクロ111により与えられる。データの中に入って行われる図解は図11に示す共心の四角形で表してある。消費者アクセスマクロもしくは消費者ビューは、その消費者もしくはデータ主体に関するデータを収容する消費者データベースの単一行へのアクセスをユーザー/消費者に与える。システムアシスタント1102がデータベースのインフラストラクチャーの定義と管理維持をサポートする一方、プライバシーアシスタント1104がそれらの表、データビュー、マクロ、ユーザープロフィール、ログ、監査レポートをサポートする。前述の場合と同様、ルーチンアプリケーション110Aは標準ビュー260を介して、また解析アプリケーション110Cは匿名ビューを介して、顧客ベース表にアクセスする。この場合、顧客の身元を同定できるデータは隠されており、処置アプリケーション（マーケティング アプリケーション）110Dは顧客データの全行が省かれる適用除外選択ビューを介してアクセスし、サードパーティ公開アプリケーション112に与えられるデータビューは、適用選択をした顧客のみを表す身元同定データへのアクセスは許可しない。適用除外選択/匿名化データビューは別個に用意したデータビューで与えることができ、あるいは適用除外選択および匿名化の両方を適用するデータビューで与えることができる。

【図面の簡単な説明】

【図1】データウェアハウス化システム実施例のシステムブロック図である。

【図2】プライバシー拡張顧客表およびデータベースビ

ュー内に格納された顧客表の構造例を示すブロック図である。

【図3】データウェアハウス化システムの別の実施例のシステムブロック図である。

【図4】本発明の特徴であるプライバシー監査オペレーションの概略を表すブロック図である。

【図5】本発明の一実施例を実行するために使用されるオペレーション例を示す流れ図である。

【図6】本発明の一実施例におけるデータベース管理システムインターフェースを介してデータへのアクセスを与えるのに使用するオペレーション例を示す流れ図である。

【図7】本発明の一実施例においてプロキシサービスリクエストを受信するために使用するオペレーション例を示す流れ図である。

【図8】データソースからのアクセスリクエストメッセージを受信するために使用するオペレーション例を示す流れ図である。

【図9】別個に設けた信託データベースを備えたプライバシーデータウェアハウスの別の実施例を示す図である。

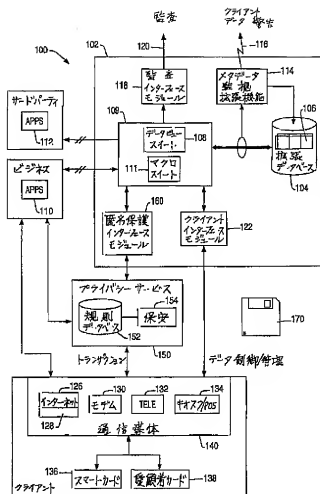
【図10】すべてのデータアクセスの管理を行いとログをとるべく介在させたプライバシーメタデータ サービスインターフェースを備えた、プライバシーデータウェアハウスの別の実施例を示す図である。

【図11】プライバシーメタデータ サービスインターフェースが介在するデータビューの実施例を示す図である。

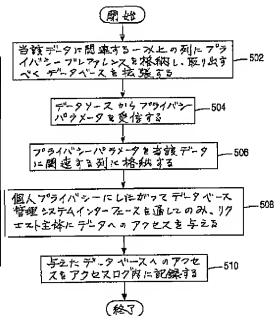
【符号の説明】

- 100 データウェアハウス化システム
- 102 保安データウェアハウス (secure data warehouse)
- 104 データベース管理システム (database management system)
- 106 拡張データベース
- 128 ブラウザプラグイン
- 202 顧客表
- 204 同定情報部分
- 206 個人情報部分
- 208 機密情報部分
- 210 グローバルデータ制御列
- 212 データ制御列
- 902 格納表
- 904 信託データベース
- 1002 プライバシーメタデータサービスインターフェース
- 1104 プライバシーアシスタント

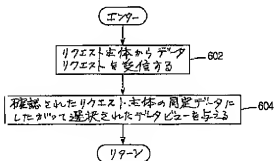
【図1】



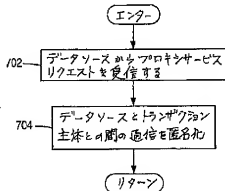
【図5】



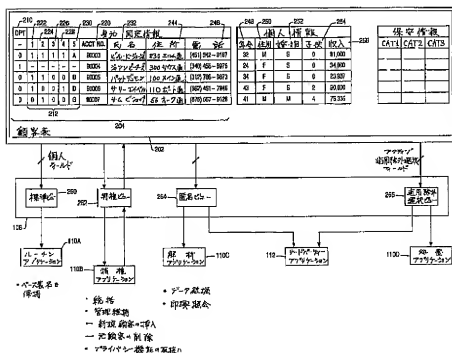
【図6】



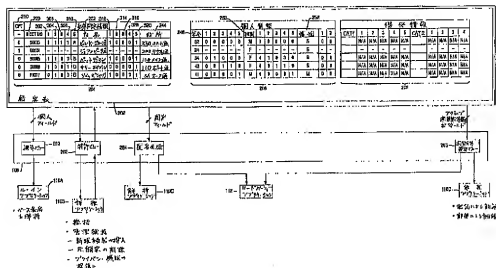
【図7】



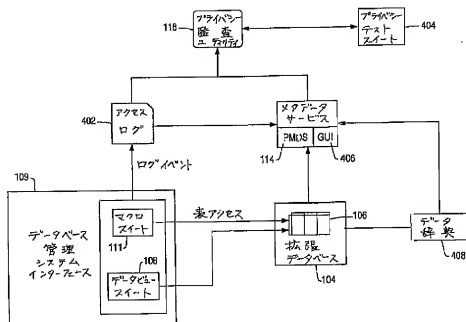
【图2】



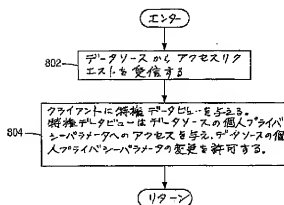
【图3】



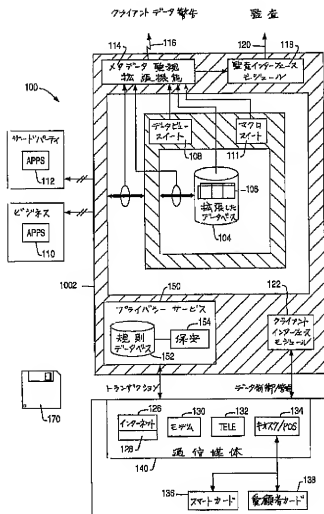
【 図 4 】



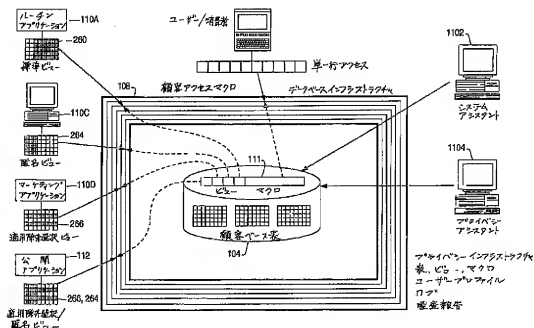
【 図 8 】



【図10】



【図11】



フロントページの続き

- (72)発明者 ケネス ダブリュー オフラハティ
アメリカ合衆国 92130 カリフォルニア
州 サン ディエゴ トリー ビュー コ
ート 3765
- (72)発明者 リチャード ジー ステルワゴン ジュニア
アメリカ合衆国 92064 カリフォルニア
州 ボーウェイ カミノ デル パーレ
13035
- (72)発明者 トッド エー ウォルター
アメリカ合衆国 92064 カリフォルニア
州 ボーウェイ ストートウッド ストリ
ート 12600
- (72)発明者 レイド エム ワッツ
アメリカ合衆国 29072 サウスキャロラ
イナ州 レキシントン スプリング クリ
ーク コート 201

- (72)発明者 デビッド アレン ラムゼイ
アメリカ合衆国 29072 サウスキャロラ
イナ州 レキシントン ベレ チェイス
ドライブ 124
- (72)発明者 アドリアン ダブリュー ベルドワイセン
アメリカ合衆国 92069 カリフォルニア
州 サン マルコス ターンベリー ドラ
イブ 1661
- (72)発明者 レンダ ケー オズデン
アメリカ合衆国 92128 カリフォルニア
州 サン ディエゴ キャンドリッジ ロ
ード 12019
- (72)発明者 バトラリック ビー デンプスター
アメリカ合衆国 07716 ニュージャージ
ー州 アトランティック ハイランズ ベ
ープ ドライブ 59